AMENDMENTS

In the Claims

The following is a marked-up version of the claims with the language that is underlined (“____”) being added and the language that contains strikethrough (“——”) being deleted:

1. (Original) A method comprising the steps of:

(A) receiving an email message from a simple mail transfer protocol (SMTP) server, the email message comprising:

(A1) a 32-bit string indicative of the length of the email message;

(A2) a text body;

(A3) an SMTP email address;

(A4) a domain name corresponding to the SMTP email address;

(A5) an attachment;

(B) tokenizing the text body to generate tokens representative of words in the text;

(C) tokenizing the SMTP email address to generate a token representative of the SMTP email address;

(D) tokenizing the domain name to generate a token that is representative domain name;

(E) tokenizing the attachment to generate a token that is representative of the attachment, the tokenizing step comprising the steps of:

(E1) generating a 128-bit MD5 hash of the attachment;

(E2) appending the 32-bit string to the generated MD5 hash to produce a 160-bit number; and

(E3) UUencoding the 160-bit number to generate the token representative of the attachment;

(F) determining a probability value for each of the generated tokens;

(G) selecting a predefined number of interesting tokens, the interesting tokens being the generated tokens having the greatest non-neutral probability values;

(H) performing a Bayesian analysis on the selected interesting tokens to generate a spam probability; and

(I) categorizing the email message as a function of the generated spam probability.

2 – 5. (Canceled)

6. (Original) A method comprising the steps of:

receiving an email message comprising a text body, an SMTP email address, and a domain name corresponding to the SMTP email address;

tokenizing the SMTP email address to generate a token representative of the SMTP email address;

tokenizing the domain name to generate a token representative of the domain name; and

determining a spam probability from the generated tokens.

7 – 10. (Canceled)

11. (Original) The method of claim 6, wherein the step of determining the spam probability comprises the steps of:

assigning a spam probability value to the token representative of the SMTP email address;

assigning a spam probability value to the token representative of the domain name; and

generating a Bayesian probability value using the spam probability values assigned to the tokens.

12. (Original) The method of claim 11, wherein the step of determining the spam probability further comprises the step of:

comparing the generated Bayesian probability value with a predefined threshold value.

13. (Original) The method of claim 12, wherein the step of determining the spam probability further comprises the step of:

categorizing the email message as spam in response to the Bayesian probability value being greater than the predefined threshold.

14. (Original) The method of claim 12, wherein the step of determining the spam probability further comprises the step of:

categorizing the email message as non-spam in response to the Bayesian probability value being not greater than the predefined threshold.

15. (Original) A method comprising the steps of:

receiving an email message comprising an attachment;

tokenizing the attachment to generate a token representative of the attachment; and

determining a spam probability from the generated token.

16. (Original) The method of claim 15, wherein the step of receiving the email message further comprises the step of:

receiving an email message including a text body.

17. (Original) The method of claim 16, further comprising the step of:

tokenizing the words in the text body to generate tokens representative of the words in the text body.

18. (Canceled)

19. (Original) The method of claim 17, wherein the step of determining the spam probability comprises the steps of:

assigning a spam probability value to each of the tokens representative of the words in the text body;

assigning a spam probability value to the token representative of the attachment; and

generating a Bayesian probability value using the spam probability values assigned to the tokens.

20. (Original) The method of claim 19, wherein the step of determining the spam probability further comprises the step of:

comparing the generated Bayesian probability value with a predefined threshold value.

21. (Original) The method of claim 20, wherein the step of determining the spam probability further comprises the step of:

categorizing the email message as spam in response to the Bayesian probability value being greater than the predefined threshold.

22. (Original) The method of claim 20, wherein the step of determining the spam probability further comprises the step of:

categorizing the email message as non-spam in response to the Bayesian probability value being not greater than the predefined threshold.

23. (Original) A system comprising:

email receive logic configured to receive an email message comprising an SMTP email address and a domain name corresponding to the SMTP email address;

tokenize logic configured to tokenize the SMTP email address to generate a token representative of the SMTP email address;

tokenize logic configured to tokenize the domain name to generate a token representative of the domain name; and

analysis logic configured to determine a spam probability from the generated tokens.

24. (Original) A system comprising:

means for receiving an email message comprising an SMTP email address and a domain name corresponding to the SMTP email address;

means for tokenizing the SMTP email address to generate a token representative of the SMTP email address;

means for tokenizing the domain name to generate a token representative of the domain name; and

means for determining a spam probability from the generated tokens.

25. (Original) A computer-readable medium comprising:

computer-readable code adapted to instruct a programmable device to receive an email message comprising an SMTP email address and a domain name corresponding to the SMTP email address;

computer-readable code adapted to instruct a programmable device to tokenize the SMTP email address to generate a token representative of the SMTP email address;

computer-readable code adapted to instruct a programmable device to tokenize the domain name to generate a token representative of the domain name; and

computer-readable code adapted to instruct a programmable device to determine a spam probability from the generated tokens.

26. (Original) The computer-readable medium of claim 25, further comprising:

computer-readable code adapted to instruct a programmable device to assign a spam probability value to the token representative of the SMTP email address;

computer-readable code adapted to instruct a programmable device to assign a spam probability value to the token representative of the domain name; and

computer-readable code adapted to instruct a programmable device to generate a Bayesian probability value using the spam probability values assigned to the tokens.

27. (Original) The computer-readable medium of claim 26, further comprising:

computer-readable code adapted to instruct a programmable device to compare the generated Bayesian probability value with a predefined threshold value.

28. (Original) The computer-readable medium of claim 27, further comprising:

computer-readable code adapted to instruct a programmable device to categorize the email message as spam in response to the Bayesian probability value being greater than the predefined threshold.

29. (Original) The computer-readable medium of claim 27, further comprising:

computer-readable code adapted to instruct a programmable device to categorize the email message as non-spam in response to the Bayesian probability value being not greater than the predefined threshold.

30. (Original) A system comprising:

email receive logic configured to receive an email message comprising an attachment;

tokenize logic configured to tokenize the attachment to generate a token representative of the attachment; and

analysis logic configured to determine a spam probability from the generated token.

31. (Original) A system comprising:

means for receiving an email message comprising an attachment;

means for tokenizing the attachment to generate a token representative of the attachment; and

means for determining a spam probability from the generated token.

32. (Original) A computer-readable medium comprising:

computer-readable code adapted to instruct a programmable device to receive an email message comprising an attachment;

computer-readable code adapted to instruct a programmable device to tokenize the attachment to generate a token representative of the attachment; and

computer-readable code adapted to instruct a programmable device to determine a spam probability from the generated token.

33. (Original) The computer-readable medium of claim 32, further comprising:

computer-readable code adapted to instruct a programmable device to receive an email message having a text body.

34. (Original) The computer-readable medium of claim 33, further comprising:

computer-readable code adapted to instruct a programmable device to tokenize the words in the text body to generate tokens representative of the words in the text body.

35. (Original) The computer-readable medium of claim 34, further comprising:

computer-readable code adapted to instruct a programmable device to assign a spam probability value to each of the tokens representative of the words in the text body;

computer-readable code adapted to instruct a programmable device to assign a spam probability value to the token representative of the attachment; and

computer-readable code adapted to instruct a programmable device to generate a Bayesian probability value using the spam probability values assigned to the tokens.

36. (Original) The computer-readable medium of claim 35, further comprising:

computer-readable code adapted to instruct a programmable device to compare the generated Bayesian probability value with a predefined threshold value.

37. (Original) The computer-readable medium of claim 36, further comprising:

computer-readable code adapted to instruct a programmable device to categorize the email message as spam in response to the Bayesian probability value being greater than the predefined threshold.

38. (Original) The computer-readable medium of claim 36, further comprising:

computer-readable code adapted to instruct a programmable device to categorize the email message as non-spam in response to the Bayesian probability value being not greater than the predefined threshold.